

CLAIMS :

1. A method of using an anti fraud card system comprising a card component and a transmitter component both physically separate and distinct from each other and comprised of a built-in battery, a CPU to handle various processes, a non-volatile memory to hold coding information, with said card component further comprising a signal strip and a receiver while said transmitter further comprising a transmitter module and having the following improvement on the method of use:

a user hands out his card to a vendor, when a vendor is about to swipe said card, said user activates a first third of a code by pressing a button sequence on a keypad; said button sequence also triggers a second third of a code and both codes are transmitted from said transmitter over to said card and said CPU inside said card processes said codes and combines it with a third part of a code contained in said card's own non-volatile memory module in order to create a complete ID code; said ID code is processed so as to be sent out to a signal strip in a recognizable pattern readable by a standard magnetic strip reader handled by said vendor; as soon as said transmitter stops sending said signal, said CPU that is in said card erases said code parts sent by said transmitter and ceases to send the signal to said signal strip to render said card unusable.

2. An anti-fraud card system as in claim 1 wherein:

said transmitter transmits an IR signal and said card receives an IR signal.

3. An anti-fraud card system as in claim 1 wherein:

when said user releases the last button, said transmitter ceases to send the signal to said signal strip to render said card unusable.

4. An anti-fraud card system as in claim 1 wherein:

when said user releases the last button, the signal continues to be sent for a preset duration.

5. An anti-fraud card system as in claim 1 wherein:

said transmitter has a keypad having three buttons.